

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
18 December 2003 (18.12.2003)

PCT

(10) International Publication Number
WO 03/105475 A1

(51) International Patent Classification⁷: **H04N 7/167, 7/173**

(21) International Application Number: **PCT/US03/17970**

(22) International Filing Date: **6 June 2003 (06.06.2003)**

(25) Filing Language: **English**

(26) Publication Language: **English**

(30) Priority Data:
60/386,867 7 June 2002 (07.06.2002) US

(71) Applicant (for all designated States except US): **GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).**

(72) Inventor; and

(75) Inventor/Applicant (for US only): **VINCE, Lawrence, D. [US/US]; 114 Aileen Drive, Lansdale, PA 19446 (US).**

(74) Agent: **LIPSITZ, Barry, R.;** Law offices of Barry R. Lipsitz, 755 Main Street, Building No. 8, Monroe, CT 06468 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

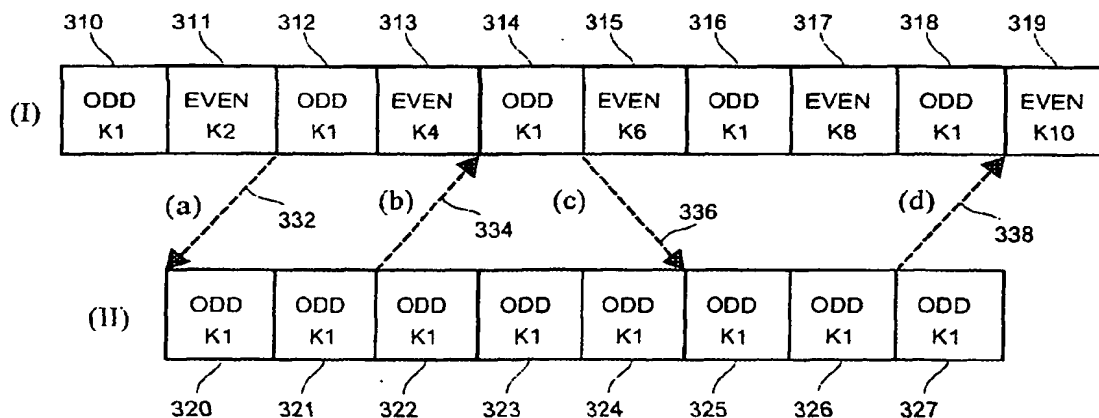
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SEAMLESS SWITCHING BETWEEN MULTIPLE PRE-ENCRYPTED VIDEO FILES



(57) Abstract: In a video on demand (VOD) system, methods and apparatus are provided for seamlessly switching back and forth between two pre-encrypted files having changing encryption keys. Such switching back and forth may be required when a VOD server stores both a "normal" copy of a movie and a "special" copy such as a "trick-play" version for, e.g., fast forward and rewind effects. Instead of using keys with changing parities in both streams, the special stream is encrypted with keys using the same parity (even or odd), while the normal stream is encrypted with one dynamic key (odd or even) and one fixed key (even or odd). Other special streams, such as scene branch streams and alternate angle streams can also be accommodated.

WO 03/105475 A1

SEAMLESS SWITCHING BETWEEN MULTIPLE PRE-ENCRYPTED VIDEO FILES

This application claims the benefit of U.S. provisional application no. 60/386,867 filed on June 7, 2002, which is incorporated herein and made a part hereof by reference.

TECHNICAL FIELD OF THE INVENTION

The present invention relates to copy protection techniques and more particularly to encryption for interactive, on-demand digital program content such as video-on-demand (VOD) program material (files) which is delivered (streamed) over cable television, satellite television, and other wired or wireless broadband communications networks.

BACKGROUND OF THE INVENTION

Video On Demand

Video On Demand (VOD) is an interactive application offered on a digital television (DTV) network, other movie network, or the like. VOD is made practical by broadband digital broadcasting via cable and satellite. Unlike earlier services where subscribers were granted access only to scheduled encrypted broadcasts (e.g., movie channels, special events programming, etc.), these "on-demand" services permit a subscriber to request a desired video, audio or other programming at any time. Upon receiving the request for programming (and, presumably, authorization to bill the subscriber's account), the service provider then transmits the requested program to the subscriber for viewing. Audio On Demand provides similar functionality for sound files (versus video files). In the main hereinafter, VOD is discussed.

The Motion Picture Association of America (MPAA) is a trade association of the American film industry, whose members include the industry's largest content providers (i.e., movie producers, studios). The MPAA requires protection of VOD content from piracy. Without security to protect the content, the member content providers will not release their content (e.g., movies) for VOD distribution. Without the up-to-date, high-quality content, the VOD market becomes non-viable.

For content providers and operators, the need for a secure VOD solution is therefore necessary. Two different approaches can be selected - either "pre-encryption," or "encryption at playout." Pre-encryption means that the content is encrypted before being stored (as a file) on the video server, the goal being to encrypt the content as soon as possible, for example as soon as it leaves the production studio. Pre-encryption is well suited to programming material having fixed content, such as movies, and is generally preferred for interactive applications. Encryption at playout means that the content is encrypted in real time, and is suitable for the secure broadcasting of live events. In the main hereinafter, VOD with pre-encrypted content is discussed.

As used herein, a "file" is the video source material which is stored, preferably encrypted, and a "stream" is the digital signal derived from the file when the file is broadcast (transmitted) to end user(s).

Modern VOD services give the user control over the playout of a selected program with features functionally comparable to those of a video cassette recorder (VCR) - for example, "trick play" (e.g., fast-forward, rewind, etc.). This requires that more than one file be maintained for a given program content - for example, a "normal" file and a "special" trick-play file which is associated with the normal file. The user is able to transition between the two files, interactively. Both files must, of course, be encrypted. (Again, in the main hereinafter, VOD with pre-encrypted content is discussed.)

MPEG-2

A digital TV signal is typically transmitted as a stream of MPEG-2 data, although other type streams are expected to become available in the future (e.g., MPEG-4) that are within the scope of the present invention. MPEG-2 is a method for compressed representation of video and audio sequences using a common coding syntax defined in the document ISO/IEC 13818 by the International Organization for Standardization. The MPEG-2 Video Standard specifies the coded bit stream for high-quality digital video.

The MPEG standard defines a transport stream (TS) for transmitting data from one or more MPEG streams. Each transport stream (TS) has a data rate of up to 40 megabits per second, which is enough for seven or eight separate TV channels/programs (also referred to as services). Each transport stream consists of a set of sub-streams

(known as elementary streams), where each elementary stream can contain either MPEG-2 encoded audio, MPEG-2 encoded video, or data encapsulated in an MPEG-2 stream. A multiplexer assigns a packet identifier (PID) to each elementary stream, and splits the elementary streams into transport packets which are inserted into a transport stream (TS).

- 5 The multiplexer can combine several MPEG streams into a single transport stream (TS).

MPEG-2 accommodates scrambling at the elementary stream level and/or at the transport stream level. The MPEG-2 specification contains a scrambling control field of two bits, both in the TS packet header and in the PES packet header. Generally, the first scrambling control bit indicates whether or not the payload is scrambled (encrypted), and
 10 the second scrambling control bit indicates the use of Even or Odd Key, as follows:

Bit Values	Description
00	No scrambling of packet payload
01	Reserved for future DVB use
10	Packet scrambled with even key
11	Packet scrambled with odd key

Encryption Schemes

Present encryption schemes typically employ a simple two-key encryption scheme to encrypt VOD content. Both keys taken together are essentially a single “cryptographic key set” used to encrypt the entire content. One of the keys comprises one or more
 15 “public keys” delivered with the content. The other key is required in combination with the public key(s) to decrypt the content, and is delivered as part of a successful authorization or licensing process. Neither key is useful absent the other key.

A problem with encrypting the VOD content with a single set of “public keys” is that an aggressive “attack” using exhaustive cryptographic “cracking” techniques could
 20 discover a pair of keys that will decode the content. Once broken, the content can be reproduced “in the clear” (i.e., unencrypted), thereby completely thwarting the security offered by the encryption scheme.

For highest security and greatest protection against cryptographic "cracking" attacks by "pirates", it is highly desirable to increase the number of separate cryptographic keys used by changing the keys at numerous points during the encryption process. In other words, it is generally highly desirable to encrypt VOD files with frequently changing cryptographic keys. According to the MPEG-2 standard, when packets are encrypted with a changing key, it is necessary to toggle between even and odd parity key numbers.

Pre-encryption of video (e.g., MPEG-2) files is a cost effective method for enabling security for movies and other types of pre-recorded files. However, the pre-encryption of video when using more than two encryption keys has been problematic in the past. In particular, when it is desired to switch back and forth between two or more pre-encrypted files (such as a normal file and a special trick play mode file that provides, e.g., fast forward or rewind), it is very difficult to maintain encryption key synchronization (key sync). This problem can cause errors during decryption in the decoder, and has negatively impacted the introduction and ability to provide satisfactory and cost effective video on demand (VOD) services with trick play modes. The problem manifests itself when the normal file that is being played back is encrypted with an even (or odd) parity key choice and navigation moves to playback of a trick play (e.g., fast forward or rewind) file where the pre-encryption key is also an even (or odd) choice, yet different from the key that was used in the normal file. The same problem can occur when moving (transitioning, navigating) back from the trick play file to the normal file.

In the past, real time encryption has been proposed to solve this problem. However, real time encryption requires substantial hardware resources in order to function acceptably, and therefore carries a significant cost.

GLOSSARY

Unless otherwise noted, or as may be evident from the context of their usage, any terms, abbreviations, acronyms or scientific symbols and notations used herein are to be given their ordinary meaning in the technical discipline to which the invention most nearly pertains. The following glossary of terms is intended to lend clarity and consistency to the various descriptions contained herein, as well as in prior art documents:

ECM	Entitlements Control Message. Entitlement Control Messages are private conditional access information which specify control words and possibly other, typically stream-specific, scrambling and and/or control parameters.
EMM	Entitlements Management Message. Conditional access messages used to convey entitlements or keys or other parameters to users, or to invalidate or delete entitlements or keys. For example, an EMM can be used in combination with an ECM to determine an encryption key.
ER	Encryption Record. Contains information about how specific program content is encoded, rules for decoding, etc.
ERS	ECM Renewal System
MPEG	Moving Pictures Experts Group
MPEG-2	MPEG-2 is the standard for digital television (officially designated as ISO/IEC 13818, in 9 parts).
MSO	Multiple System Operator. A company that owns multiple cable television systems.
OLEs	Off-Line Encryption Station

PES	Packetized Elementary Stream
STB	Set Top Box. An electronic device that allows a television (TV) set to connect to the Internet, game systems, cable television systems or satellite television systems.
TS	Transport Stream
VOD	Video-On-Demand. The service of providing content through subscriber selection off a large menu of options, available to a viewer at any time.

SUMMARY OF THE INVENTION

According to the invention, in a video on demand (VOD) system, methods and apparatus are provided for seamlessly switching back and forth between two pre-encrypted files having changing encryption keys. Such switching back and forth may be required when a VOD server stores both a "normal" copy of a movie and a "special" copy such as a "trick-play" version for, e.g., fast forward and rewind effects. The invention addresses and overcomes problems associated with using encryption keys having changing parities in both streams.

In an embodiment of the invention, instead of using keys with changing parities in both streams, the normal stream is encrypted with one dynamic key (odd or even) and one fixed key (even or odd), and the special stream is encrypted with keys having the same parity (even or odd). Other special streams, such as scene branch streams and alternate camera angle streams can also be accommodated.

Typically, special streams (files) which are related to or associated with the normal stream are processed. If the special stream (file) were completely unrelated, then there might be other aspects of switch back and forth that would make the transitions non-seamless. The general intent of the present invention is to allow the encryption to take place on top of seamless transitions so that the encryption does not cause undue side effects. Also, when pre-encrypting, the files are grouped together so that they can be encrypted with a common key set. Without this 'pre-grouping' of content (thus causing a relationship), pre-encryption potential degrades to the point where 'every packet would be encrypted with the same key', which is not desired.

Additionally, it should be understood that having a fixed key rather than a changing key for the trick play file represents an acceptable 'compromise.' The overall intent is to protect the totality of the content. Trick play files are usually just snippets of the video (e.g., a collection of stills) with either no audio or significantly modified audio. As such, this material is not generally very interesting to a hacker, pirate or counterfeiter.

The present invention provides a technique for allowing VOD navigation between two (or more) files, without requiring real time encryption. Instead of providing real-time encryption, the key sync problem is solved by applying a minor restriction on pre-

encryption that does not significantly adversely impact the security of the data. More specifically, methods and apparatus are provided for pre-encrypting video files with normal rate and trick play (e.g., fast-forward / rewind) files to make switching (transitioning) between the files as seamless as possible when more than two keys are
5 used for encryption. The disclosed techniques are also useful for switching between normal files and other types of files, such as scene branch files, alternate camera angle files, or other special files that are desired to be switched with a file containing plain (i.e., normal) video. The invention also solves the problem of ping-ponging between two files where the MPEG encryption parity bit may be the same.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a system for delivering pre-encrypted video content.

Figure 2 is a diagram illustrating how packets are transported in accordance with the MPEG2 standard without consideration of the side effects of switching between two files, according to the prior art.

Figure 3 is a diagram illustrating a modified approach to pre-encrypting content in accordance with a preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to copy protection techniques and, more particularly, to copy protection for interactive, on-demand digital program content such as video-on-demand (VOD) programming distributed (e.g.) via cable and satellite networks.

5 In order to protect against interception and copying of digital program content, it is known to use a pre-encryption scheme whereby server-based VOD content is stored in an encrypted form, then delivered directly to viewers without further encryption processing. The VOD content is encrypted at the point where it is encoded, and is distributed to content resellers (e.g., MSOs, satellite operators, etc.) in encrypted form.
10 Content encoders generally do not distribute directly to end-users (viewers). Typically, encryption is accomplished separately and uniquely for each reseller.

Figure 1 is a block diagram of a system 100 for delivery of pre-encrypted program content. At a content encoder's location 110, master content 112 (e.g., movies and other program content) is encoded into digital form via a MPEG-2 encoder 114. This
15 content is then encrypted in an encryption system 116. A content authorization system 118 is used to manage, renew and verify valid licensing for the encrypted content, permitting encryption by the encryption system 116 only if valid licensing exists for any particular destination. The encryption system 116 generates a "personalized" encryption for each destination content reseller (e.g., MSO). The encrypted content is transmitted
20 via a transmitter 120 over a suitable transmission medium 140 (satellite shown, but can be Internet, cable, or any other suitable delivery mechanism) to a receiver 132 at a reseller's location. The receiver 132 receives the encrypted content and stores it in a VOD server 134 from which it can be re-broadcast to end-users. A system manager 136 (computer system that controls operation of a reseller's various transmission and communications
25 resources) communicates with the encryption system 116 to make requests for program content, and to receive encryption records (ER) defining how the requested program content is encrypted/encoded and to receive entitlement control messages (ECMs) associated with the encryption of the program content. Typically, the encryption system 116 and the system manager 136 are parts of an ECM Renewal System (ERS) by which
30 authorizations to distribute/decode program content are managed and renewed.

At the reseller's (e.g., MSO's) location, a user authorization system receives requests from end users for program content and verifies that appropriate authorizations are in place for the end user to view the requested content. If they are, then the user authorization system instructs the VOD server to deliver the requested (encrypted) content to the user's VOD playback device 150 (e.g., set-top box) and generates an Entitlements Management Message (EMM) for the requested content for delivery to the VOD playback device 150 along with the requested content.

An entitlements control message (ECM) contains encryption information about the encryption specific to the program content which, in combination with a valid entitlements management message (EMM), can be used to derive an encryption key for decoding the content. ECMs are typically embedded within the program content and due to the encryption mechanisms employed, cannot be used to derive valid encryption keys absent a valid EMM for the content. EMMs also include conditional access information, such as information about when, how many times, and under what conditions the content may be viewed/played.

A technique that can be used to improve the security of encrypted streaming content such as VOD content is to change the cryptographic keys (encryption keys) at a plurality of points within the content. In order to make it more difficult for "pirates" to steal these keys, it is desirable to use as many different cryptographic keys as possible used to encrypt a program's content.

Figure 2 illustrates a situation wherein two MPEG-2 files (I) and (II) have been pre-encrypted for broadcast, each using more than one encryption key (K). For purposes of this discussion, the two files (I) and (II) are related to each other. For example, the file (I) is a normal (standard) program (service) and the other file (II) is a special "trick-play" (TP) version (e.g., fast forward and rewind effects) of the normal file (I). With VOD, the user is interactively able to transition between the two files (I) and (II).

The first file (I) comprises a sequence of groups (one or, more typically, multiple sequential ones) 210, 211, 212, 213, 214, 215, 216, 217, 218, 219 of MPEG-2 transport packets. The second file (II) comprises a sequence (one or, more typically, multiple sequential ones) 220, 221, 222, 223, 224, 225, 226, 227 of MPEG-2 transport packets.

The second file (II) is suitably a special trick play file which is associated with the first file (I) which is a normal file.

In the first file (I), the first group 210 has (is assigned) an odd key number K1, the second group 211 has an even key number K2, the third group 212 has an odd key number K3, the fourth group 213 has an even key number K4, the fifth group 214 has an odd key number K5, the sixth group 215 has an even key number K6, the seventh group 216 has an odd key number K7, the eighth group 217 has an even key number K8, the ninth group 218 has an odd key number K9, and the tenth group 218 has an even key number K10. This fulfills the condition of the MPEG-2 standard that when packets are encrypted with a changing key, it is necessary to toggle between even and odd parity key numbers.

In the second file (II), the first group 220 has (is assigned) an odd key number K19, the second group 221 has an even key number K20, the third group 222 has an odd key number K21, the fourth group 223 has an even key number K22, the fifth group 224 has an odd key number K23, the sixth group 225 has an even key number K24, the seventh group 226 has an odd key number K25, and the eighth group 227 has an even key number K26. This fulfills the condition of the MPEG-2 standard that when packets are encrypted with a changing key, it is necessary to toggle between even and odd parity key numbers.

The user is able to interactively transition between the two files (I) and (II). Four types of transitions 232, 234, 236, 238 are possible, and are illustrated.

(a) 232, moving from an even key in the normal file (I) to an even key in the TP file (II).

(b) 234, moving from an even key in the TP file (II) to an odd key on the normal file (I).

(c) 236, moving from an odd key in the normal file (I) to an odd key in the TP file (II).

(d) 238, moving from an odd key in the TP file (II) to an even key in the normal file (I).

According to the MPEG-2 standard, when packets are encrypted with a changing key, it is necessary to toggle between even and odd parity key numbers. In the case

where only two keys are used, and the key numbers (designated as even and odd) actually denote only those two keys, no problem exists. This is due to the fact that a switch is being made either between two even keys that are the same (transition 232 (a)), two odd keys that are the same (transition 236 (c)), or an odd/even transition is occurring between two keys that have already been calculated (transitions 234 (b) & 238 (d)).

In a more general case where each key number identifies a unique key (as illustrated in Figure 2), several problems can arise. One problem is that the VOD server (e.g., 134) has to identify, ahead of time, which entitlement control message (ECM) to send that will allow the proper key to be generated by the decryption processor. If the next key number is always guaranteed to be of the opposite parity (odd or even) than the current key, and the MPEG-2 transport packets are marked appropriately, then this technique will work. However, in the case where the key number is changing at some rate in both the normal stream (I) and the trick play stream (II) there is no way to guarantee that when keys are changed they will always be of opposite parity. Without such a guarantee, switching between two different keys of the same parity (transitions 232 and 236) can occur. This can result in a "race condition" between key calculation and key application that cannot be solved, except in very specific cases. The MPEG-2 transport identifies odd and even parity in the Scrambling Control bits, to avoid exactly this race condition. According to the invention, a technique is provided for switching between two different keys of the same parity, without causing such a race condition.

An example of a specific case, such as is referred to in the previous paragraph, is one where both the delivery time of the ECM and the calculation and application time of the 'next' key can be guaranteed so that even key 'K2' will be switched out for even key 'K20' at exactly the right time. The magnitude of this 'right time' can be on the order of 400 microseconds with content being delivered at 3.75 Mbps. A method other than the one defined by MPEG to synchronize the key switch would have to be created.

Figure 3 illustrates an embodiment of a technique for pre-encrypting content in accordance with the invention. The technique relies on the playout of ECMs done on time (in real time), but removes the even/odd parity problem. In particular, the trick play (TP) file (II) is encrypted with only one key K1 (even or odd parity). The normal file (I) has one dynamic key (odd or even) and one fixed key (even or odd).

A fixed key is one that does not change, it is static. A dynamic key is a changing key. The rate at which the dynamic key changes is not the focus of the present invention. What is important is that the dynamic key changes during the course of playout of a file.

For purposes of this discussion, the two files (I) and (II) are related to each other.

5 For example, the file (I) is a normal (standard) program (service) and the other file (II) is a special "trick-play" (TP) version (e.g., fast forward and rewind effects) of the normal file (I). The user is interactively able to transition between the two files (I) and (II).

The first file (I) comprises a sequence of groups (one or, more typically, multiple sequential ones) 310, 311, 312, 313, 314, 315, 316, 317, 318, 319 of MPEG-2 transport

10 packets. The second file (II) comprises a sequence (one or, more typically, multiple sequential ones) 320, 321, 322, 323, 324, 325, 326, 327 of MPEG-2 transport packets. The second file (II) is suitably a special trick play file which is associated with a the first file (I) which is a normal file.

In the first file (I), the first group 310 has (is assigned) an odd key number K1, the

15 second group 311 has an even key number K2, the third group 312 has an odd key number K1, the fourth group 313 has an even key number K4, the fifth group 314 has an odd key number K1, the sixth group 315 has an even key number K6, the seventh group 316 has an odd key number K1, the eighth group 317 has an even key number K8, the ninth group 318 has an odd key number K1, and the tenth group 318 has an even key

20 number K10. This fulfills the condition of the MPEG-2 standard that when packets are encrypted with a changing key, it is necessary to toggle between even and odd parity key numbers.

In the second file (II), the first group 320 has (is assigned) an odd key number K1, the second group 321 has an odd key number K1, the third group 322 has an odd key

25 number K1, the fourth group 323 has an odd key number K1, the fifth group 324 has an odd key number K1, the sixth group 325 has an odd key number K1, the seventh group 326 has an odd key number K1, and the eighth group 327 has an odd key number K1. Since K1 of first file (I) = K1 of second file (II), this means that because the key isn't changing in the trick play file (it is the defined 'odd' key in use), the MPEG2 payload

30 encryption bits also are always the same. The segments in file (II) denote the acceptable

entry points into the file. MPEG-2 I frames take up more than one transport packet and because of this, entry into the (II) file is restricted to specific entry points.

Generally stated, the technique illustrated in Figure 3 comprises encrypting the first file (I) according to a first encryption scheme and encrypting the second file (II) according to a second encryption scheme. In the described embodiment, the first encryption scheme has a fixed key alternating with a changing key, and the second encryption scheme uses a fixed key which has the same parity as the fixed key of the first encryption scheme.

It should be understood that it is possible, but not preferred, that the second/special/trick file would have more than one key (a changing key). It can be done, however it would place undesirable restrictions on navigating the file. For example, (1) entry and exit from the trick play file could be managed so that the key change rule is not violated. This would mean that either (a) very limited entry and exit points would be defined or (b) multiple trick play files would be encrypted in such a way that entry into a trick play file would not violate the key change rules; (2) files could be encrypted at a very high key change rate so that the opportunities for entry and exit from the trick play file were much greater, but they would still have to be managed, and it would place a greater burden on ECM delivery rates. In both of these cases, file navigation would have to be aware of the constraints of the encryption system. In contrast thereto, the present invention makes the encryption totally transparent to the file navigation.

In the system of the invention, the user is able to transition interactively between the two files (I) and (II). Four transitions are possible, and are illustrated. Assuming, for example, that the trick play file (II) is encrypted with only an odd parity key number (K1, as illustrated) and the key is static, four types of transitions 332, 334, 336, 338 are possible. These are:

(a) 332, moving from an even key in the Normal file (I) to an odd key in the TP file (II).

(b) 334, moving from an odd key in the TP file (II) to the same odd key on the Normal file (I).

(c) 336, moving from an odd key in the Normal file (I) to the same odd key in the TP file (II).

(d) 338, moving from an odd key in the TP file (II) to an even key in the Normal file (I).

Transitions 332 (a) and 338 (d) rely on playing out the ECM ahead of time so that the MPEG-2 scrambling control bits can signal when to change the decryption key.

5 Transitions 334 (b) and 336 (c) become trivial because the odd key is the same key (K1) in both cases. It is possible, in some cases, that some Access Control implementation may have to send a different ECM even in cases 2 and 3, but the actual decryption key calculated can be the same. Thus, a glitch in decryption is avoided.

It should be noted that a particular implementation may require the ECMs to be
10 unique - i.e., an ECM cannot be simply replayed to derive a key or the system disallows reuse of an ECM. However such implementations are generally required to be able to encrypt any random key to generate an ECM, so even if they have to send a 'different' ECM, the key generated by that ECM would have to be the same. An advantage of the present invention is that it is possible to just be able to store the odd key (and not
15 recalculate it) because it never changes. Some other system may not have the option to not recalculate it, but that is acceptable as long as the ECM is sent ahead of time.

An off-line encryption station (OLES) can be used to process MPEG files (e.g., from a VOD server) and encrypt them prior to being placed back on the VOD server for delivery to consumers (See, e.g., **Figure 1**). It may be preferable for the OLES to encrypt
20 the normal file first. A predefined indication (such as, for example, a data tag or header bit) can be used to indicate that a trick play file is appended to the normal file. After encryption of the normal file, the trick play file is encrypted and appended to the normal file. In this manner, encryption of an entire movie or the like can be efficiently completed.

25 It should be understood that the order in which the files are pre-encrypted is somewhat arbitrary, and based largely on convenience. Under normal circumstances, it may be simply be easier to tack on the trick play file at the end of the normal file when encrypting. The invention is not limited by the order in which the files are encrypted.

It should be appreciated that numerous modifications and adaptations may be
30 made in accordance with the present invention. For example, the normal file can be encrypted using a dynamic key stream of one parity alternating with a fixed key of the

opposite parity, while the trick play file is encrypted with a fixed key having either the even or the odd key. The reason for this is when a transition occurs, it either has to be a different parity or the key has to be the same exact key. Other modifications and adaptations will be apparent to those skilled in the art.

What is claimed is:

1. A method for pre-encrypting video on demand (VOD) content which includes a first video file and at least one second video file, comprising:
encrypting the first video file using a fixed key having a first parity alternating with a dynamic key having a second parity opposite the first parity; and
encrypting the at least one second video file using a fixed key having a fixed parity.
2. A method in accordance with claim 1, wherein:
the fixed parity is the first parity.
3. A method in accordance with claim 1, further comprising:
alternately providing the first and second files to a user as video streams in response to the user interactively transitioning between the first and second files.
4. A method in accordance with claim 1, wherein:
the first video file is a normal video file; and
the second video file is a special trick play file associated with the normal video file.
5. A method in accordance with claim 1, wherein:
the first video file is a normal video file; and
the second video file is a scene branch file.
6. A method in accordance with claim 1, wherein:
the first video file is a normal video file; and
the second video file is an alternate camera angle file.
7. A method in accordance with claim 1, wherein a plurality of second video files are provided and encrypted.

8. A method in accordance with claim 7, wherein:
the first video file is a normal video file; and
at least one of the plurality of second video files is a special trick play file associated with the normal video file.
9. A method in accordance with claim 7, wherein:
the first video file is a normal video file; and
at least one of the plurality of second video files is a scene branch file.
10. A method in accordance with claim 7, wherein:
the first video file is a normal video file; and
at least one of the plurality of second video files is an alternate camera angle file.
11. A method for delivery of pre-encrypted program content comprising:
encoding master content into digital form;
encrypting the master content;
storing the encoded, encrypted content in a VOD server from which it can be broadcast, on demand, to end-users; wherein:
the master content comprises a first file and a second file which is associated with the first file;
the first file is encrypted according to a first encryption scheme;
the second file is encrypted according to a second encryption scheme that is different from the first encryption scheme; and
in response to a request from an end-user, delivering the encoded, encrypted content to the end-user.
12. A method in accordance with claim 11, wherein:
the first encryption scheme comprises at least two keys; and
the second encryption scheme comprises one of the at least two keys.

13. A method in accordance with claim 11, wherein:
one of the at least two keys is a changing key.
14. A method in accordance with claim 11, wherein:
one of the at least two keys is a fixed key.
15. A method in accordance with claim 11, wherein:
one of the at least two keys is a fixed key; and
the second encryption scheme uses the fixed key.
16. A method in accordance with claim 11, wherein:
the master content is encoded using the MPEG-2 standard.
17. A method in accordance with claim 11, wherein:
the first file is a normal file; and
the second file is a trick play file.
18. A method in accordance with claim 11, wherein:
the second file is appended to the first file.
19. A method in accordance with claim 11, wherein:
the second file is encrypted after the first file is encrypted.
20. A method in accordance with claim 11, wherein:
the first file is a normal file;
the second file is a trick play file;
the second file is encrypted after the first file is encrypted; and
the encrypted second file is appended to the encrypted first file.

1 / 2

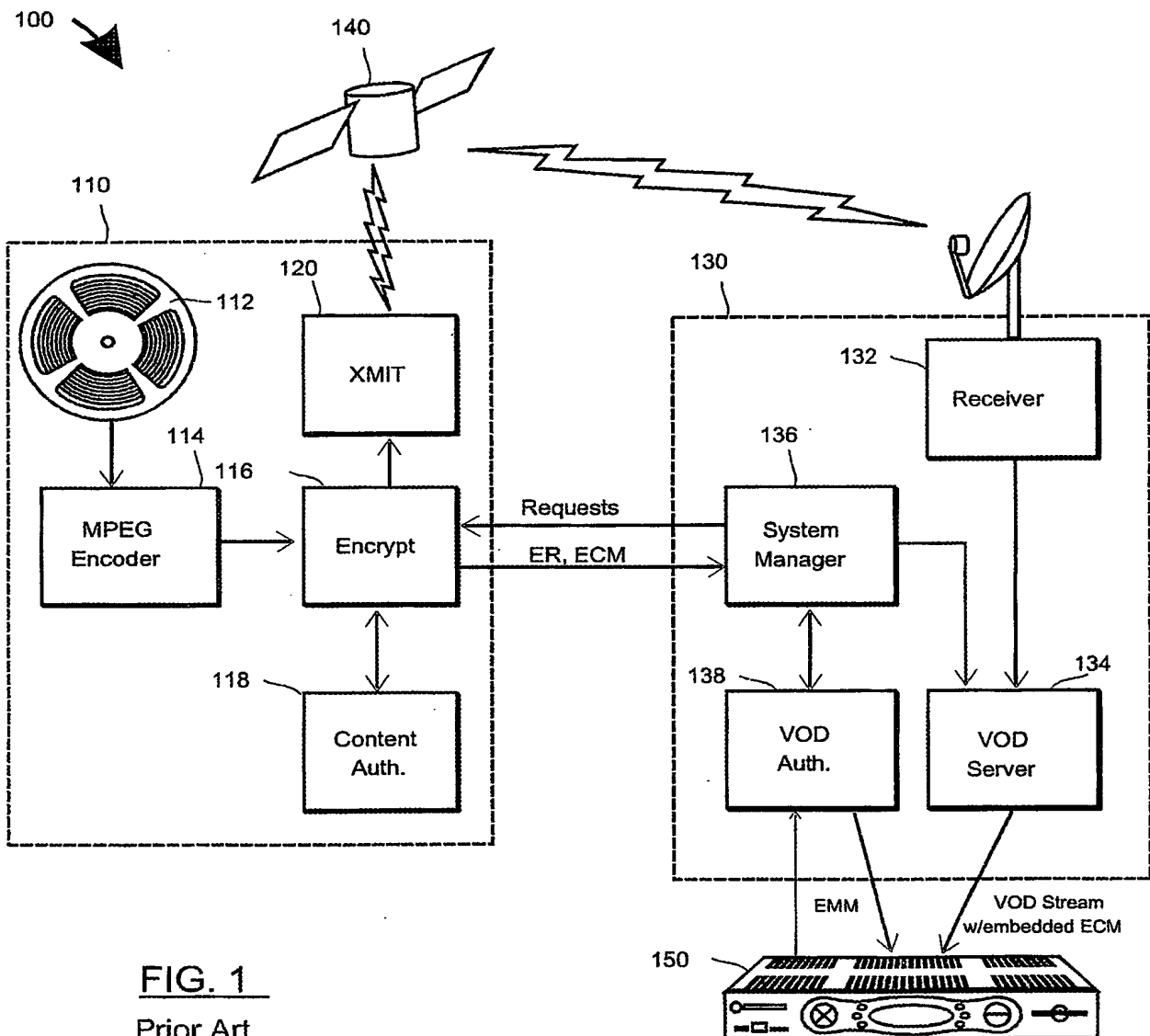


FIG. 1
Prior Art

2 / 2

FIG. 2
Prior Art

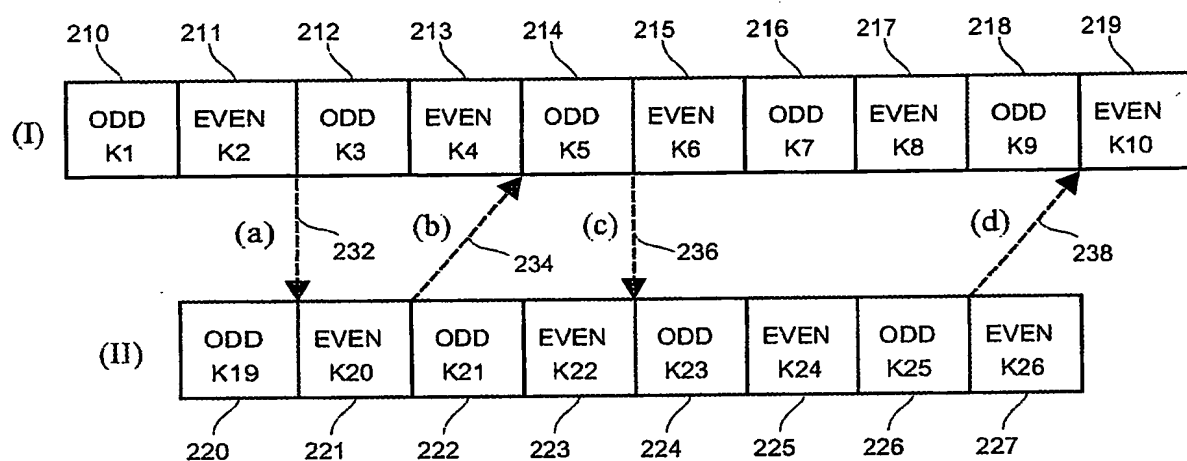
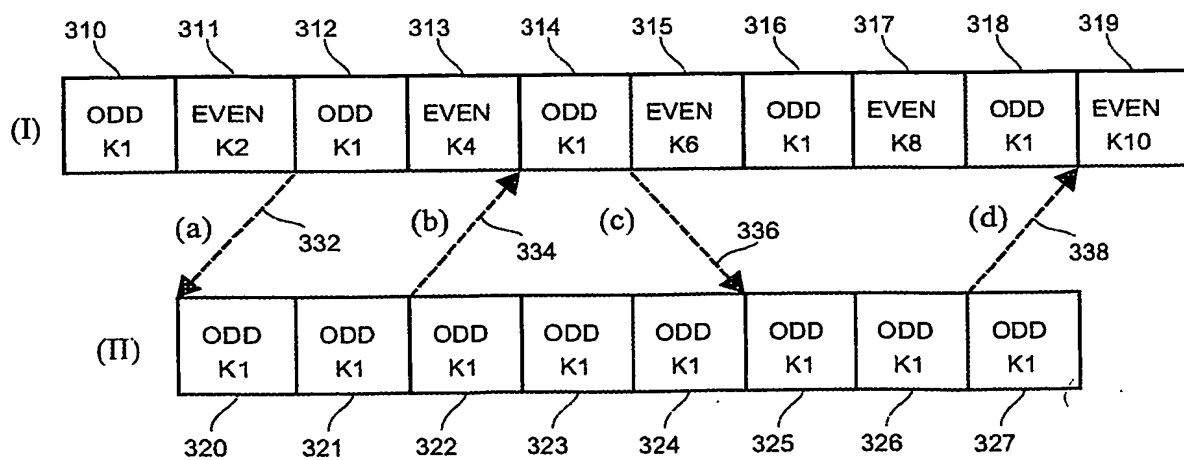


FIG. 3



INTERNATIONAL SEARCH REPORT

International Application No
PCT/JP 03/17970

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04N7/167 H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02 15579 A (GEN INSTRUMENT CORP ; SO NICOL CHUNG PANG (US)) 21 February 2002 (2002-02-21) abstract	11-13, 16-20
A	page 1, line 26 -page 3, line 26 page 6, line 8 -page 6, line 14 page 7, line 4 -page 7, line 23 page 11, line 8 -page 11, line 22 ---	1-10, 14, 15
A	WO 01 15448 A (GEN INSTRUMENT CORP) 1 March 2001 (2001-03-01) abstract page 4, line 4 -page 4, line 21 page 5, line 1 -page 5, line 23 page 12, line 11 -page 13, line 11 ---	1-20
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

23 September 2003

Date of mailing of the international search report

09/10/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Schoeyer, M

INTERNATIONAL SEARCH REPORT

International Application No

PCT/JP 03/17970

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 742 681 A (GUILLOU LOUIS ET AL) 21 April 1998 (1998-04-21) column 5, line 26 -column 8, line 42 -----	1-20
A	EP 1 022 900 A (SONY CORP) 26 July 2000 (2000-07-26) abstract paragraph '0150! - paragraph '0175! -----	1-20
A	ATSC: "Guide to the use of the ATSC Television Standard" ADVANCED TELEVISION SYSTEMS COMMITTEE, 'Online! 4 October 1995 (1995-10-04), pages 1-136, XP002255337 Retrieved from the Internet: <URL:www.atsc.org/standards/a_54.pdf> 'retrieved on 2003-09-23! -----	1-20
A	page 80, paragraph 8.4 -page 82, paragraph 8.4.2.1 -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/JP 03/17970

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0215579	A	21-02-2002	WO 0215579 A1	21-02-2002
			AU 4814400 A	25-02-2002
			CA 2408232 A1	21-02-2002
			EP 1275250 A1	15-01-2003
WO 0115448	A	01-03-2001	AU 7068200 A	19-03-2001
			BR 0013522 A	07-05-2002
			CA 2382701 A1	01-03-2001
			CN 1378744 T	06-11-2002
			EP 1206877 A1	22-05-2002
			JP 2003507974 T	25-02-2003
			WO 0115448 A1	01-03-2001
US 5742681	A	21-04-1998	FR 2718594 A1	13-10-1995
			DE 69505652 D1	03-12-1998
			DE 69505652 T2	17-06-1999
			EP 0754391 A1	22-01-1997
			WO 9528058 A1	19-10-1995
			NO 963995 A	06-12-1996
EP 1022900	A	26-07-2000	WO 0003541 A1	20-01-2000
			EP 1022900 A1	26-07-2000